What is claimed is:

1. A cryptographic method using dual keys in a wireless local area network (LAN) system, comprising:

(a) generating a first group key in N wireless terminals forming an ad-hoc group, where N is equal to or greater than two;

(b) generating a second group key in a main wireless terminal to perform a key distribution center function among the N wireless terminals, and transmitting the second group key to (N-1) sub wireless terminals; and

(c) encoding data using the second group key, and transmitting the encoded data between the N wireless terminals.

2. The method as claimed in claim 1, wherein the first group key is generated using a group password of the ad-hoc group.

3. The method as claimed in claim 1, wherein in (b), the main wireless terminal encodes the second group key using the first group key, and transmits the encoded second group key to the (N-1) wireless terminals.

4. The method as claimed in claim 1, wherein the main wireless terminal is a creator of the ad-hoc group.

5. The method as claimed in claim 1, wherein when the main wireless terminal is withdrawn from the ad-hoc group, the main wireless terminal transfers a function of key distribution center to a sub wireless terminal selected from among the (N-1) sub wireless terminals, so that the sub wireless terminal acts as the main wireless terminal.

6. The method as claimed in claim 1, further comprising:

(d) modifying the second group key in the main wireless terminal according to a predetermined modification time period, and transmitting the modified second group key to the (N-1) sub wireless terminals.

7. The method as claimed in claim 6, wherein in (d), the modified second group key is encoded using a non-modified second group key, and transmitting the encoded second group key to the (N-1) sub wireless terminals.

8. The method as claimed in claim 1, wherein (b) comprises:

(b1) if the first group key is created, encoding a second group key request message from one of the (N-1) sub wireless terminals, and transmitting the encoded second group key request message to the main wireless terminal;

(b2) decoding the second group key request message, using the first group key, in the main wireless terminal; and

(b3) creating a second group key according to the decoded second group key request message, in the main wireless terminal.

9. A computer readable medium having embodied thereon a computer program for the method according to claim 1.

10. A computer readable medium having embodied thereon a computer program for the method according to claim 3.

11. A computer readable medium having embodied thereon a computer program for the method according to claim 8.

12. A wireless local area network (LAN) system, comprising:

N, where N is equal to or greater than two, wireless terminals which form an ad-hoc group, and create a first group key, wherein the N wireless terminals include:

a main wireless terminal for performing a key distribution center function in the ad-hoc group, for creating a second group key and encoding data using the second group key, and for transmitting the encoded data between the remaining wireless terminals; and

(N-1) sub wireless terminals for receiving the second group key from the main wireless terminal and encoding data using the second group key, and for transmitting the encoded data between the remaining wireless terminals.

13. The system as claimed in claim 12, wherein the first group key is generated using a group password of the ad-hoc group.

14. The system as claimed in claim 12, wherein the main wireless terminal encodes the second group key using the first group key, and transmits the encoded second group key to the (N-1) wireless terminals.

15. The system as claimed in claim 12, wherein the main wireless terminal is a creator of the ad-hoc group.

16. The system as claimed in claim 12, wherein when the main wireless terminal is withdrawn from the ad-hoc group, the main wireless terminal transfers a function of key distribution center to a sub wireless terminal selected from among the (N-1) sub wireless terminals, so that the sub wireless terminal acts as the main wireless terminal.

17. The system as claimed in claim 12, wherein the sub wireless terminal comprises:

a first group key generator for creating a first group key using a group password input from a user;

a first encryption unit for storing the first group key, for encoding a second group key request message, using the first group key, for decoding a second group key response message from the main wireless terminal using the first group key, and for encoding data input from a user using a second group key; and

a first key management unit for generating the second group key request message to output to the first encryption unit, for extracting a second group key from the second group key response message decoded in the first encryption unit, and for outputting the extracted second group key to the first encryption unit.

18. The system as claimed in claim 12, wherein the main wireless terminal comprises:

a second group key generator for creating a first group key using a group password input from a user;

a second encryption unit for storing the first group key, for decoding the second group key request message transmitted from the sub wireless terminal using the first group key, for encoding the second group key

response message for transmitting to the sub wireless terminal using the first group key, and for encoding data input from a user using the second group key; and

a second key management unit for receiving the second group key request message decoded from the second encryption unit, for creating the second group key, and for outputting the second group key response message including the created second group key to the second encryption unit.

19. The system as claimed in claim 18, wherein the second key management unit modifies the second group key according to a predetermined modification time period, and transmits the modified second group key to each of the (N-1) sub wireless terminals.

20. The system as claimed in claim 19, wherein the second encryption unit encodes the modified second group key using a non-modified second group key, and transmits the encoded modified second group key to each of the (N-1) sub wireless terminals.